Aspects of Voting Machine Software Testing at PTB

1. Manual code inspections

(list not complete)

- Inspection of the code parts which deal with the general operation of the machine:
    - checks that the activation of the voting machine by polling staff is implemented in a secure way, and that there is no other way to activate the machine;
    - examination of the conditions under which the polling staff is allowed to withdraw activation;
    - checks that the automatic de-activation of voting machine after voting is implemented in a secure way, and that there a no ways to get around de-activation;
    - examination of the conditions under which the voting machine accepts inputs from voters and polling staff;
    - examination of the conditions under which the voting machine displays reminders and asks for confirmation;
    - checks that the outputs (for example, lights and/or beeps) correspond to the inputs;
    - check that identification names and numbers are treated in a secure way, and handled without modifications, and that all checksums are computed correctly;
    - examination of all functions which compute and transport the election results (counting errors, possible overflow, modifications on transport, ...).

- Inspection of the code parts for voter input:
    - checks that all variables are of sufficient type and size, that they are initialised and resetted in case of errors, or when the voter finishes voting or corrects his decision, or when the polling staff withdraws activation;
    - examination of the way the value of a pressed key is processed and converted into a vote;
    - examination of the conditions under which the voting machine adds null votes and examination of the way the voting machine distinguishes null votes from normal votes;
    - checks of the paths the vote is transported through the software;
    - checks that the vote is displayed, printed, stored into ballot module, and put into COM messages without unallowed modifications;
    - checks that the reading of a vote corresponds to the writing.

- Inspection of the code parts for key and display management:

    - checks that the voting machine correctly reads the content of the ballot module (table of keys and candidates);
    - check that all keys and key codes are distinct;
    - check that all passive keys are blocked in a secure way, and examination of the conditions under which blocked keys may be activated again;
    - check that the displays and lights correspond to the voters inputs;
    - examination of the kind of information which is displayed at the voting machine and at the control unit in normal case and in error case.

- Inspection of the code parts for ballot and backup modules:

    - collection of all reading and writing accesses to ballot and backup modules, and check that all write accesses at polling day are acceptable;
    - checks that the information is read out and written correctly;
    - examination of the conditions under which the content of ballot and backup modules are changed;
    - check that the backup module is a true copy of the ballot module and that otherwise the polling staff is informed.

- Inspection of the code parts for control and error handling:

    - collection and analysis of all security measures for the vote storage process; and check, that the number of stored votes is always correct;
    - check that each erroneous situation is registered and treated in a right way; and that each error is written into error memory, and presented to voter or polling staff in an appropriate way;
    - inspection of the code written to treat power losses and the emergency storage of votes in that case;
    - collection of all conditions, which may inhibit vote storage;
    - check that all parts of hardware and software are checked at startup time, and that problems lead to a blocking of the voting machine or ballot module;
    - check that the most important parts of hardware and software are checked permanently at run time, and that problems lead to a blocking of the voting machine or ballot module;
    - check that changes of the software may be detected;
    - check that changes of the ballot module may be detected;
    - check that incorrect operation by the voter or polling staff does not result in problems for the voting process, and that incorrect operation by voter and polling staff is always recoverable.

- Inspection of all code to confirm that the voting machine implements only functions which are necessary for voting.

2. Dynamic function tests

On several functions, to support or replace code inspection; based on software tools.

3. Static analyses

Analyses of the source code based on software tools.

4. Integration tests (on the machine)

Check that the operation of the voting machine is as specified concerning:

- activation of the machine by polling staff, automatic de-activation, and withdrawal of activation by polling staff;
- all operations of the voter to select a vote on any ballot paper, to correct his decisions, and to end the voting process with no votes, less votes, or enough votes;
- all invalid operations which are possible;
- print outputs, displays, and beeps, including the clearing of displays in case of errors or corrections;
- all steps done in preparation of a voting day and to close a voting day.

All modules are checked (roughly).

5. Inspection of the tests at the manufacturers

All test documents are inspected:

- check that the most important functions are tested;
- check that the test cases are sufficient;
- check that the expected results and the test results are plausible.

Subject to test are the modules as tested by the manufacturer.

6. Examinations on successive versions

If primary version of software is re-engineered by the manufacturer according to problems:

- the successive version is checked for differences (file compare), the differences are analysed, and inspections to be done again are selected;
- the lists of problems reported to the manufacturer are checked.

All relevant modules are subject to test.

7. Inspection of software documentation

8. Audit of the software development processes at the manufacturers